ON THE NUMBER OF SOLUTIONS OF DECOMPOSABLE FORM INEQUALTITIES

C.L.Stewart

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

Debrecen number theory seminar,November 22, 2024

Let n be an integer with $n \geq 2$ and put $\mathbf{X} = (X_1, ..., X_n)$. Let F be a non-zero decomposable form in n variables with integer coefficients and degree d with $d > n$, so

$$F(\mathbf{X}) = L_1(\mathbf{X})....L_d(\mathbf{X}) \tag{0.1}$$

where $L_1(\mathbf{X}), ..., L_d(\mathbf{X})$ are linear forms in $\mathbb{C}[X_1, ..., X_n]$.

Norm forms, discriminant forms, index forms and binary forms are examples of decomposable forms.
Note that $L_1(\mathbf{X}), ..., L_d(\mathbf{X})$ are not uniquely determined by F since if $\alpha_1, ..., \alpha_d$ are complex numbers with

$$\alpha_1....\alpha_d = 1$$

then $F(\mathbf{X}) = H_1(\mathbf{X})...H_d(\mathbf{X})$ when

$$\alpha_i L_i(\mathbf{X}) = H_i(\mathbf{X})$$

for $i = 1, ..., d$.

Let m be a positive integer and let $N_F(m)$ denote the number of points $(a_1, ..., a_n)$ with integer coordinates for which

$$|F(a_1, ..., a_n)| \leq m. \tag{0.2}$$

Let V_F denote the volume of the set

$$\{(x_1, ..., x_n) \in \mathbb{R}^n : |F(x_1, ..., x_n)| \leq 1\}.$$

By homogeneity the volume of

$$\{(x_1, ..., x_n) \in \mathbb{R}^n : |F(x_1, ..., x_n)| \leq m\} \tag{0.3}$$

is $V_F m^{n/d}$ and one might suppose that $N_F(m)$ is close to $V_F m^{n/d}$.

When is that so?

F is said to be of *finite type* if V_F is finite and the same is true for F restricted to any non-trivial rational subspace. In particular, for every n'-dimensional subspace S of $\mathbb{R}^n$ defined over $\mathbb{Q}$ the n'-dimensional volume of F restricted to S is finite.

In 2001 Thunder showed that if F is of finite type then

$$N_F(m) \ll_{n,d} m^{n/d}; \tag{0.4}$$

the symbol $\ll$ together with a subscript means less than a positive number which depends on the terms in the subscript. Thunder's result resolved a conjecture of Schmidt and is best possible up to the dependence of the implicit constant on n and d.

For any element $\mathbf{x} = (x_1, ..., x_n)$ in $\mathbb{C}^n$ let $\|\mathbf{x}\| = (x_1\overline{x}_1 + ... + x_n\overline{x}_n)^{1/2}$. For any linear form $L(\mathbf{X}) = \alpha_1 X_1 + ... + \alpha_n X_n$ in $\mathbb{C}[X_1, ..., X_n]$ let **L** denote the coefficient vector $(\alpha_1, ..., \alpha_n)$ of $L(\mathbf{X})$. We define the quantity $\mathcal{H}(F)$ of F by

$$\mathcal{H}(F) = \prod_{i=1}^{d} \|\mathbf{L}_i\| .$$

Thunder also proved that if F is of finite type and F is not proportional to a power of a definite quadratic form in 2 variables then there exist positive numbers a_F and c_F such that

$$|N_F(m) - m^{n/d} V_F| \ll_{n,d} \mathcal{H}(F)^{c_F} (1 + \log m)^{n-2} m^{\frac{n-1}{d-a_F}}. \qquad (0.5)$$

If the discriminant of the form is non-zero then one may take $a_F = 1$ and $c_F = \binom{d-1}{n-1} - 1$.

In 1933 Mahler proved that if $n = 2$ and $F(X_1, X_2)$ is a binary form with integer coefficients which is irreducible over the rationals then

$$|N_F(m) - m^{2/d} V_F| \ll_F m^{1/(d-1)}. \tag{0.6}$$

Thunder's result is a generalization of (0.6) since if F is irreducible over $\mathbb{Q}$ then $a_F = 1$ and F is of finite type.

Ramachandra, in 1969, was the first to obtain an asymptotic result for $N_F(m)$ for a class of decomposable forms with $n \geq 3$. He did so when F has the shape

$$F(\mathbf{X}) = N_{\mathbb{K}/\mathbb{Q}}(X_1 + \alpha X_2 + \alpha^2 X_3 + ... + \alpha^{n-1} X_n)$$

where $\mathbb{K} = \mathbb{Q}(\alpha)$ is a number field of degree r with $r \geq 8n^6$ and $N_{\mathbb{K}/\mathbb{Q}}$ denotes the norm from $\mathbb{K}$ to $\mathbb{Q}$.

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and put $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Suppose that $F(\mathbf{X})$ is a norm form so

$$F(\mathbf{X}) = N_{\mathbb{K}/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_n X_n) = \prod_{\sigma} \sigma(\alpha_1 X_1 + \ldots + \alpha_n X_n)$$

where the product is taken over the isomorphic embeddings σ of $\mathbb{K}$ into $\mathbb{C}$.

Let V be the vector space of all rational linear combinations of $\alpha_1, ..., \alpha_n$. For each subfield $\mathbb{J}$ of $\mathbb{K}$ we define the linear subspace $V^{\mathbb{J}}$ of V given by the elements of V which remain in V after multiplication by any element of $\mathbb{J}$. F is said to be non-degenerate if $\alpha_1, ..., \alpha_n$ are linearly independent over $\mathbb{Q}$ and if $V^{\mathbb{J}} = \{0\}$ for each subfield $\mathbb{J}$ of $\mathbb{K}$ which is not $\mathbb{Q}$ or an imaginary quadratic field.

In 1972 Schmidt proved that $N_F(m)$ is finite for each positive integer m if and only if F is non-degenerate. In 2000 Evertse proved that if F is a non-degenerate norm form then

$$N_F(m) \leq (16d)^{(n+1)^3/3}(1+\log m)^{n(n-1)/2} m^{(n+\sum_{m=2}^{n-1} 1/m)/d}. \quad (0.7)$$

Non-degenerate norm forms are of finite type and so (0.4) gives a better dependence on m than (0.7) although the dependence of the upper bound on n and d is not explicit in (0.4).

Let $N_F^*(m)$ denote the number of vectors $(a_1, ..., a_n)$ with integer coordinates for which

$$0 < |F(a_1, ..., a_n)| \le m. \tag{0.8}$$

If F is of finite type then F does not vanish at any non-zero integer point and so

$$N_F(m) = 1 + N_F^*(m). \tag{0.9}$$

There exist distinct irreducible polynomials $F_1, ..., F_k$ with integer coefficients, content 1 and degrees $d_1, ..., d_k$ respectively and there exist positive integers $l_1, ..., l_k$ for which $d_1 l_1 + ... + d_k l_k = d$ such that

$$F(\mathbf{X}) = C_0 F_1(\mathbf{X})^{l_1} ... F_k(\mathbf{X})^{l_k}, \tag{0.10}$$

where $|C_0|$ is the content of F.

For each integer j with $1 \leq j \leq k$ the polynomial $F_j(\mathbf{X})$ is of the form $aN_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X}))$ where a is a non-zero rational number, $\mathbb{K}$ is a number field of degree d_j over $\mathbb{Q}$, $N_{\mathbb{K}/\mathbb{Q}}$ denotes the norm from $\mathbb{K}$ to $\mathbb{Q}$ and $L(\mathbf{X})$ is a linear form which is proportional to a linear form L_i with i from $\{1, ..., d\}$.

For $i = 1, ..., d$ let B_i be the rational subspace of $\mathbb{R}^n$ for which $L_i(\mathbf{X}) = 0$. Note that if $L_i(\mathbf{X})$ and $L_j(\mathbf{X})$ divide $F_h(\mathbf{X})$ in $\mathbb{C}[\mathbf{X}]$ for some h with $1 \leq h \leq k$ then $B_i = B_j$. Thus each polynomial $F_i(\mathbf{X})$ determines exactly one rational subspace of $\mathbb{R}^n$, say A_i, for which $F_i(\mathbf{X}) = 0$.

Put

$$d_F = \begin{cases} 0 & \text{if } A_i = \{\mathbf{0}\} \text{ for } \ i = 1, ..., k \\ \max\{l_{i_1} d_{i_1} + ... + l_{i_j} d_{i_j}\} & \text{otherwise,} \end{cases} \tag{0.11}$$

where the maximum is taken over those tuples $(i_1, ..., i_j)$ of distinct integers for which $A_{i_1} \cap ... \cap A_{i_j}$ is different from the zero vector or equivalently for which there is a non-zero integer point $(s_1, ..., s_n)$ for which $F_{i_m}(s_1, ..., s_n) = 0$ for $m = 1, ..., j$.

F is said to be of *essentially finite type* if V_F is finite, $V(\tilde{F})$ is finite whenever $\tilde{F}$ is F restricted to a rational subspace of $\mathbb{R}^n$ which is not a subspace of A_i for $i = 1, ..., k$ and

$$A_1 \cap ... \cap A_k = \{\mathbf{0}\}. \tag{0.12}$$

If F is of essentially finite type then, by virtue of (0.12) ,

$$d_F < d. \tag{0.13}$$

Further, if F is of finite type then it is also of essentially finite type since in this case $A_i = \{\mathbf{0}\}$ for $i = 1, ..., k$ and so (0.12) holds.

Theorem

Let $F(\boldsymbol{X})$ be a non-zero decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ and let m be a positive integer. If F is of essentially finite type then

$$N_F^*(m) \ll_{n,d} m^{\frac{1}{d} + \frac{n-1}{d-d_F}}. \tag{0.14}$$

Notice that if F is of finite type then $d_F = 0$ and Thunder's result (0.4) follows from (0.9) and (0.14).

The proof of Theorem 1 depends on a quantitative version of Schmidt's Subspace Theorem due to Evertse. A key feature of Theorem 1 is that the upper bound for $N_F^*(m)$ is independent of the coefficients of the form F. We require such an estimate in order to prove the analogue of Thunder's second estimate estimate (0.5) for forms of essentially finite type.

Before stating such a result we shall make explicit the quantities a_F and c_F.

For a factorization as in (0.1) of F we let $I(F)$ denote the set of all n-tuples $(\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_n})$ of linearly independent coefficient vectors. For each linear form $L_i(\mathbf{X})$ from (0.1) we denote by $b(L_i)$ the number of n-tuples in $I(F)$ which contain $\mathbf{L}_i$ and we put

$$b_F = \max\{b(L_1), ..., b(L_n)\}.$$

Next let $J(F)$ be the subset of $I(F)$ consisting of n-tuples $(\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_n})$ for which for $j = 1, ..., n-1$ either $\mathbf{L}_{i_{j+1}}$ is proportional to $\overline{\mathbf{L}}_{i_j}$ or $\overline{\mathbf{L}}_{i_j}$ is in the span of $\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_j}$. We then put

$$a_F = \max \left\{ \frac{\text{the number of } \mathbf{L}_i \text{ in the span of } \mathbf{L}_{i_1}, ..., \mathbf{L}_{i_j}}{j} \right\}$$

where the maximum is taken over integers j from $\{1, ..., n-1\}$ and n-tuples $(\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_n})$ from $J(F)$.

Finally we put

$$c_F = \begin{cases} \binom{d-1}{n-1} - 1 & \text{if } \Delta_F \neq 0 \\ \frac{b_F}{n! a_F}(d - (n-1)a_F) - \frac{1}{a_F} & \text{otherwise.} \end{cases}$$

Theorem

Let $F(\boldsymbol{X})$ be a decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ and let m be an integer with $m > 1$. If F is of essentially finite type then

$$|N_F^*(m) - m^{n/d} V_F| \ll_{n,d} \mathcal{H}(F)^{c_F} (\log m)^{n-2} m^{\frac{n-1}{d-a_F}}$$

$$+ (\log m + \log \mathcal{H}(F))^{n-1} m^{\frac{1}{d} + \frac{n-2}{d-d_F}} (0.15)$$

If F is of finite type then $d_F = 0$ and $a_F \geq 1$. Thus

$$\frac{1}{d} + \frac{n-2}{d-d_F} = \frac{n-1}{d} < \frac{n-1}{d-a_F}$$

and so Thunder's second result (0.5) follows from Theorem 2.

For the proof we appeal to Theorem 1 and, once again, to a quantitative version of the Subspace Theorem.

If F is of essentially finite type and F is not proportional to a power of a definite quadratic form in 2 variables then

$$1 \leq a_F \leq \frac{d}{n} - \frac{1}{n(n-1)}. \tag{0.16}$$

The discriminant Δ_F of a form as in (0.1) is given by

$$\Delta_F = \prod_{(i_1,\ldots,i_n)} det(\mathbf{L}_{i_1}^{tr}, \ldots, \mathbf{L}_{i_n}^{tr})$$

where the product is taken over all n-tuples of distinct integers $(i_1, \ldots, i_n)$ with $1 \leq i_j \leq d$ for $j = 1, \ldots, n$. Here $\mathbf{L}^{tr}$ denotes the transpose of $\mathbf{L}$.

Let $B(x, y)$ denote the Beta function. In 1996 Bean and Thunder proved that if $\Delta_F \neq 0$ then

$$|\Delta_F|^{\frac{(d-n)!}{d!}} V_F \leq C_n \tag{0.17}$$

where

$$C_n = \frac{2}{n} \prod_{k=1}^{n-1} \left(B(\frac{1}{n+1}, \frac{k}{n+1}) + B(\frac{n-k}{n+1}, \frac{k}{n+1}) + B(\frac{n-k}{n+1}, \frac{1}{n+1}) \right);$$

the case when $n = 2$ was established by Bean in 1994.

They proved that the upper bound of C_n is sharp in (0.17) and that C_n grows like a constant times $(2n)^n$.

If Δ_F is non-zero then $a_F = 1$ and $c_F = \binom{d-1}{n-1} - 1$. Thus by Theorem 2 and (0.17) we have the following result.

Corollary

Let $F(\boldsymbol{X})$ be a decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ and let m be an integer with $m > 1$. If F is of essentially finite type and $\Delta_F \neq 0$ then

$$N_F^*(m) \ll_{n,d} m^{n/d}|\Delta_F|^{-\frac{(d-n)!}{n!}} + \mathcal{H}(F)^{\binom{d-1}{n-1}-1}(\log m)^{n-2} m^{\frac{n-1}{d-1}}$$

$$+ (\log m + \log \mathcal{H}(F))^{n-1} m^{\frac{1}{d}+\frac{n-2}{d-d_F}} (0.18)$$

When $n = 2$, $F(\mathbf{X})$ is a binary form and if Δ_F is non-zero then F is of essentially finite type and d_F is either 0 or 1. Since $a_F = 1$ we obtain our next result.

Corollary

Let $F(\boldsymbol{X})$ be a binary form with integer coefficients, degree d with $d \geq 3$ and $\Delta_F \neq 0$. Let m be a positive integer. Then

$$|N_F^*(m) - m^{2/d} V_F| \ll_d m^{\frac{1}{d-1}} \mathcal{H}(F)^{d-2}. \tag{0.19}$$

Corollary 4 generalizes Mahler's result (0.6), where F is assumed to be irreducible over the rationals, to the case where F has a non-zero discriminant. By (0.5) such a result holds when F is of finite type but that does not give Corollary 4 in the case when F has a linear factor over the rationals.

The proofs of Theorems 1 and 2 build on the work of Thunder. He proceeds by establishing an upper bound for each $\mathbf{x}$ in $\mathbb{R}^n$ for

$$\frac{\prod_{j=1}^{n} |L_{i_j}(\mathbf{x})|}{|det(\mathbf{L}_{i_1}^{tr}, ..., \mathbf{L}_{i_n}^{tr})|}$$

for some n-tuple $(\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_n})$ from $I(F)$. Thunder establishes two such estimates.

Let $F(\mathbf{X})$ be a decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ as in (0.1).

LEMMA

If $F(\boldsymbol{X})$ is of essentially finite type and F is not proportional to a power of a definite quadratic form in 2 variables then there is a positive number $C_1 = C_1(n, d)$, which depends on n and d, such that for every $\boldsymbol{x} \neq \boldsymbol{0}$ in $\mathbb{R}^n$ there is an n-tuple $(\boldsymbol{L}_{i_1}, ..., \boldsymbol{L}_{i_n})$ in $J(F)$ for which

$$\frac{\prod_{j=1}^{n} |L_{i_j}(\boldsymbol{x})|}{|det(\boldsymbol{L}_{i_1}^{tr}, ..., \boldsymbol{L}_{i_n}^{tr})|} \leq C_1 \left(\frac{|F(\boldsymbol{x})|}{\|\boldsymbol{x}\|^{d-na_F}} \right)^{1/a_F} \mathcal{H}(F)^{c_F}.$$

The preceding Lemma was proved by Thunder when F is of finite type.

Let $I'(F)$ be the subset of $I(F)$ consisting of the n-tuples $(\mathbf{L}_{i_1}, ..., \mathbf{L}_{i_n})$ of linearly independent coefficient vectors with $i_1 < i_2 < ... < i_n$.

Lemma

If $F(\boldsymbol{X})$ is of essentially finite type and $\mathcal{H}(F)$ is minimal among forms equivalent to F then there is a positive number $C_2 = C_2(n,d)$, which depends on n and d, such that for every $\boldsymbol{x}$ in $\mathbb{R}^n$ there is an n-tuple $(\boldsymbol{L}_{i_1},\ldots,\boldsymbol{L}_{i_n})$ in $I'(F)$ and there is a polynomial $G(\boldsymbol{X})$ in $\mathbb{Z}[\boldsymbol{X}]$ of degree d_0, with $d_0 \geq d - d_F$, which divides $F(\boldsymbol{X})$ in $\mathbb{Z}[\boldsymbol{X}]$ for which

$$\frac{\prod_{j=1}^{n} |L_{i_j}(\boldsymbol{x})|}{|det(\boldsymbol{L}_{i_1}^{tr},\ldots,\boldsymbol{L}_{i_n}^{tr})|} \leq C_2 \frac{|F(\boldsymbol{x})|^{1/d} |G(\boldsymbol{x})|^{\frac{n-1}{d_0}}}{\mathcal{H}(F)^{1/d}}.$$

If T is in $\mathrm{GL}_n(\mathbb{Z})$ then the form $G(\mathbf{X}) = F(T(\mathbf{X}))$ is said to be equivalent to F. Then $V_F = V_G$ but $\mathcal{H}(F)$ need not be equal to $\mathcal{H}(G)$. Put

$$\mathcal{H}_0(F) = \min_T \mathcal{H}(F \circ T)$$

where the minimum is taken over T in $\mathrm{GL}_n(\mathbb{Z})$.

In 1989 Schmidt established a quantitative version of the Subspace Theorem . This was subsequently refined by Evertse in 1996. By combining Lemma 5 with the result of Evertse we are able to prove the following result.

Lemma

Let F be a decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ as in (0.1). Suppose that F is of essentially finite type and that F is not proportional to a power of a definite quadratic form in 2 variables. Put

$$C = max(C_1, m^{\frac{1}{a_F}}, m^{\frac{1}{d}}\mathcal{H}_0(F)^{1+c_F})^{4a_F(n-1)} \qquad (0.20)$$

where C_1 is given in Lemma 5. There is a positive number c, which is computable in terms of n and d, and there are t proper rational subspaces $T_1, ..., T_t$ of $\mathbb{Q}^n$ with $t \leq c$ such that if $\boldsymbol{a}$ is an integer point with $\|\boldsymbol{a}\| \geq C$ for which

$$1 \leq |F(\boldsymbol{a})| \leq m$$

then $\boldsymbol{a}$ is in $T_1 \cup ... \cup T_t$.

Suppose F is proportional to a power of a definite quadratic form in 2 variables, say

$$F(X_1, X_2) = h(AX_1^2 + BX_1X_2 + CX_2^2)^k \tag{0.21}$$

with h, k, A, B, C integers with $h \neq 0, k \geq 2$ and $B^2 - 4AC < 0$.

LEMMA

Then

$$|N_F^*(m) - \frac{2\pi}{\sqrt{4AC - B^2}}(\frac{m}{h})^{2/d}| \ll (\frac{m}{h})^{1/d}. \qquad (0.22)$$

In 1915 Landau gave an asymptotic estimate for $N_G(m)$, hence also for $N_G^*(m)$, when $G(X_1, X_2) = AX_1^2 + BX_1X_2 + CX_2^2$ however he did not make explicit the dependence on the coefficients of G in his estimate, a feature that we require.

Thank you for your attention.